10 tips to protect yourself from social media scams.

A recent study from Gallup shares that teens spend an average of 4.8 hours on social media every day. But it's not just teens … more and more people outside this age demographic are on social media, compared to just a few years ago. This increased usage means social media has become a breeding ground for scams.

On top of being a hassle, being scammed on social media can lead to financial, identity, and other safety concerns. That's why it's important to know what tactics scammers are using, how you can spot scams, and what you can do today to be proactive and reduce your risk.

Follow these 10 tips to help stay safe from social media scams:

1. **Look for suspicious behavior from friends.** Unusual online activity from a friend or a post containing a suspicious link could indicate a compromised account. Reach out to your friend over the phone or text (not via the app) to verify a post is legitimate before clicking any links or interacting with it.

2. **Keep an eye out for grammar and a sense of urgency.** Things like capitalized phrases, misspellings, excessive punctuation, and extreme emoji use can be telltale signs of scams. Scammers often use shock factors, fear, and urgency to get you to take action and lure clicks. If a post looks or sounds off or is too good to be true, it is likely a scam. Trust your gut.

3. **Use multi-factor authentication (MFA).** This two-step login approach adds an extra layer of security when you're logging into social media accounts. MFA will prompt you to provide additional verification before logging in, like answering a security question or inputting a text code, making it more difficult for scammers to compromise your account. However, scammers are always looking for

new angles and are targeting MFA users, too. So, take precautions and remember that support personnel from the platform will never ask you for your MFA code.

4. **Set your social media accounts to private.** When your social pages are widely accessible, cybercriminals may try targeting you, specifically, in what's known as a spear phishing attack. Let's say you post about your passion for a certain charity or hobby. Since that information is available to strangers, someone could reach out pretending to be a member of such an organization with the intention of scamming you, warns KnowBe4.

5. **Think before you post.** The more detail you post, the more susceptible to crime you may be. In addition to setting your social media accounts to private, avoid posting things like the names of your pets, your birthday, your maiden name, photos containing house numbers, vacation locations, etc. Additionally, avoid posting when you're going on vacation or taking an extended leave from home. Criminals also keep a watchful eye on social media for home burglary opportunities.

6. **Don't reply to someone you don't know.** It could be a friend of a friend … or it could be a cybercriminal. Direct messages are common spots for phishing, so be alert in social media messages. KnowBe4 shares, "Some cybercriminals will even use online bots to reply to your posts or message you automatically."

7. **Only download apps from trusted publishers.** Anyone can publish an app on the app store. If you're downloading a new social media platform, look for the publisher's information, the number of reviews, and overall legitimacy of the app before downloading anything to your phone.

8. **Pause before making in-app purchases.** In-platform shopping continues to grow in popularity. If you click out to another website or page, do a thorough check before inputting your credit card information, like going to Google and searching for customer reviews or the Better Business Bureau rating. If you're purchasing through a marketplace, ask if the seller can text you a verification code before you send any payment through. This will help prove their legitimacy and protect you from selling scams.

9. **Look yourself up.** A couple times each year, look yourself up on social media apps or through an online search. See if anyone is using your name, photos, or other content to impersonate you.

10. **Shut down old accounts.** Scammers often look for old accounts with low activity and outdated passwords to hack. Is there a social platform you no longer find yourself using? Consider shutting it down and deleting it from your phone to protect yourself and the people in your network.

Social media scams may continue to rise, so being social media wise is your best defense. Looking for even more peace of mind? Talk to one of our local, independent agents today.